

**UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS**

WINSTON CASEY, RICK HAUSS and  
SANDY HAUSS on behalf of themselves  
and all others similarly situated,

Plaintiffs,

v.

TARGET CORPORATION,  
Defendant.

Civil Action No.

**CLASS ACTION COMPLAINT**

Plaintiffs Winston Casey (“Casey”) Rick Hauss (“R. Hauss”) and Sandy Hauss (“S. Hauss”) (“Plaintiffs”) bring this class action against Defendant Target Corporation (“Target” or “Defendant”), on behalf of themselves and all others similarly situated to obtain damages, restitution, and injunctive relief for the Classes, as defined below, from Defendant. Plaintiffs, for their class action complaint, allege as follows upon personal knowledge as to themselves and their own acts and experiences, and as to all other matters, upon information and belief, including investigation conducted by their attorneys.

**I. NATURE OF ACTION**

1. A nationwide breach in Target’s point-of-sale retail credit/debit card processing network and computer system and/or “cardholder data environment” compromised personal and financial data (the “Personal Information”) connected to about 40 million Target customers’ credit and debit card accounts between November 27 and December 15, 2013 – during the height of the holiday shopping season. This was the second largest of such events in U.S. history, surpassed only by a 2005 breach involving retailer TJX that affected 45.7 million card users.

2. As a result of the breach, millions of customers who shopped at a Target “brick and mortar” store anywhere in the United States between November 27, 2013 and December 15, 2013 and paid by credit or debit card had their personal and financial information breached. Many of these customers have already reported that hackers have made unauthorized charges to their accounts, and many more such unauthorized transactions are expected in the coming weeks and months.

3. Not only did Target utterly fail to live up to its duty to protect its customers’ private financial information, but Target’s response to this massive security breach has also been woefully inadequate. Target did not inform its customers of the breach for a *full four days* after discovering the hackers, and when it did report on the breach, it initially did so only on Target’s corporate website, not the commercial website frequented by Target customers. Target was so terrified of scaring off customers during the busy holiday shopping season that it failed to properly inform the millions of customers whose personal financial information had been stolen as a result of Target’s negligence.

4. On information and belief, Plaintiffs’ names and private personal financial information was among the Personal Information compromised in the data breach.

## **II. PARTIES**

5. Plaintiff Casey is an individual residing in Randolph, Massachusetts. Plaintiff Casey is a regular shopper at Target stores. Casey used his Citibank Visa debit card to purchase merchandise at the Target store in Braintree, Massachusetts on or about November 30, 2013.

6. Plaintiffs R. Hauss and S. Hauss are individuals residing in Cincinnati, Ohio. The Hausses are regular shoppers at Target stores. R. Hauss and S. Hauss used their Communication Arts Credit Union debit MasterCard to purchase merchandise at the Target

store on Colerain Avenue in Cincinnati, Ohio, on or about November 29, December 11, and December 12, 2013.

7. Defendant Target Corporation is organized under the laws of Minnesota, with a principal place of business at 1000 Nicollet Mall, Minneapolis, Minnesota 55403. Target has annual revenue of \$72 billion, with 1,797 stores throughout the United States.<sup>1</sup> Target is publicly traded under the symbol TGT.

### **III. JURISDICTION AND VENUE**

8. This Court has original jurisdiction pursuant to 28 U.S.C. §1332(d)(2). In the aggregate, Plaintiffs' claims and the claims of the other members of the Classes exceed \$5,000,000 exclusive of interest and costs, and there are numerous Class members who are citizens of states other than Target's state of citizenship, which is Minnesota.

9. This Court has personal jurisdiction over Defendant pursuant to G.L. c. 223A, § 3(a) because: (i) Defendant regularly transacts and has transacted business in the Commonwealth of Massachusetts by selling products and services to Massachusetts customers; (ii) Defendant has committed torts within the Commonwealth of Massachusetts; (iii) Defendant solicits business within the Commonwealth of Massachusetts; and (iv) the acts or conduct that are the subject matter of this action arose from Defendant's transaction of business in Massachusetts.

10. Venue is proper in this Court pursuant to 28 U.S.C. §1391 because: (i) many of the acts and transactions giving rise to this action occurred in this District; (ii) Target operates retail store locations in this District; and (iii) Plaintiff Casey resides in this District.

---

<sup>1</sup> Bloomberg. *Target Corp (TGT:New York)*, retrieved from <http://investing.businessweek.com/research/stocks/people/person.asp?personId=174446&ticker=TGT> on December 24, 2013.

#### IV. COMMON ALLEGATIONS OF FACT

11. Credit card companies require merchants to comply with Payment Card Industry (“PCI”) Data Security Standards as well as their own specific requirements, *i.e.*, Visa Operating Regulations. The basic tenets of data security in the context of credit card processing are embodied in PCI Data Security Standards 1.3.5: **“Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet”** and 1.2: **“Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.”**<sup>2</sup>

12. A massive breach of a retailer’s cardholder data environment and wide scale release of Personal Information, such as the one that affected Target during 19 of the busiest shopping days of the year, would not have occurred absent the retailer’s failure to comply with these and dozens of other Data Security Standards.

13. Target failed to exercise the care it owes to Plaintiffs and the other Class members – namely, safeguarding its cardholder data environment and securing their Personal Information.

14. News of the widespread data breach was first published by Brian Krebs, a security expert writing for “Krebs on Security,” an “in-depth security news and investigation” blog, on or about December 18, 2013 at 2:33 PM<sup>3</sup>:

According to sources at two different top 10 credit card issuers, the breach extends to nearly all Target locations nationwide, and involves the theft of data stored on the magnetic stripe of cards used at the stores.

---

<sup>2</sup> Payment Card Industry Standards Council. *Payment Card Industry (PCI) Data Security Standards, ROC Reporting Instructions for PCI DSS v2.0*. September 2011, retrieved from [https://www.pcisecuritystandards.org/documents/PCI\\_DSS\\_2.0\\_ROC\\_Reporting\\_Instructions.pdf](https://www.pcisecuritystandards.org/documents/PCI_DSS_2.0_ROC_Reporting_Instructions.pdf) on December 24, 2013.

<sup>3</sup> Krebs, Brian. *Sources: Target Investigating Data Breach*. December 13, 2012, retrieved from <http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/> on December 23, 2013.

Minneapolis, Minn. based Target Brands Inc. has not responded to multiple requests for comment. Representatives from MasterCard and Visa also could not be immediately reached for comment.

Both sources said the breach was initially thought to have extended from just after Thanksgiving 2013 to Dec. 6. But over the past few days, investigators have unearthed evidence that the breach extended at least an additional week — possibly as far as Dec. 15. According to sources, the breach affected an unknown number of Target customers who shopped at the company's bricks-and-mortar stores during that timeframe.

15. The day after Krebs broke the story, a flood of national mainstream media reports followed. By December 19, 2013, Target's negligence was fully exposed by all of the major news outlets. For example, CBS and Reuters reported<sup>4</sup>:

Target shoppers have been victims of a stunning theft of information on their credit and debit card accounts in recent days.

The giant retailer said Thursday about 40 million credit and debit card accounts may have been impacted in U.S. stores between Nov. 27 and Dec. 15, 2013.

16. Target's response to the incident was woefully inadequate. The company claims that it learned of the breach on December 15, but Target waited until December 19 -- *four full days* -- before making *any attempt* to notify customers whose Personal Information was compromised. In fact, Target announced the breach *after* Krebs did.

17. Target's website presently states<sup>5</sup>:

**What was the issue?**

The malware was discovered on our point-of-sale systems in our U.S. stores on December 15. At that time, we disabled the malicious code and immediately began notifying our card processors and the payment card networks.

18. The breach occurred during the busy holiday shopping season, a time when virtually every retailer in the United States is focused on generating as much revenue as possible. The days between Thanksgiving and Christmas comprise the period most valuable for

---

<sup>4</sup> CBS/Reuters. *Target confirms massive credit, debit card data breach*. December 19, 2012, retrieved from <http://www.cbsnews.com/news/target-confirms-massive-credit-debit-card-data-breach/> on December 23, 2013.

<sup>5</sup> Target.com. *payment card issue FAQ*, December 22, 2013, accessed from <https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ#q5881> on December 24, 2013.

retailers such as Target. Of such significance is this time period that the term “black Friday” was coined to describe the day after Thanksgiving as the most important shopping day of the year, when retailers’ accountants are finally able to mark entries in black ink as opposed to red. While Target’s belated disclosure of the data breach may have helped its bottom line, millions of its customers were left unaware that their Personal Information had been compromised.

19. Target’s belated disclosures regarding the security breach and theft of Plaintiffs’ and the other Class Members’ Personal Information were disingenuous and incomplete. On December 19, 2013, Target finally released a statement concerning the data breach, but not one designed to notify affected customers directly. Instead, Target posted a statement on its corporate website (not on the shopping site regularly accessed by customers), confirming “that the information involved in this incident included customer name, credit or debit card number, and the card’s expiration date and CVV (the three digit security code).”<sup>6</sup> In its statement concerning the data breach, Target claimed to have “worked swiftly to resolve the incident...” and provided general advice such as “you may obtain information from the FTC and the credit reporting agencies about fraud alerts and security freezes.”<sup>7</sup>

20. Target’s disclosures regarding the data breach were misleading because data thieves accessed more than the “three digit security code.” Target’s reference to a three digit security code is incorrect. “CVV2” or “card verification value,” is a term that Visa uses to describe the three-digit value printed on the signature panel of a payment card used to verify card not-present transactions. “Not-present” transactions are those which do not occur at retail locations.

---

<sup>6</sup> Steinhafel, Gregg. *A message from CEO Gregg Steinhafel about Target’s payment card issues*. December 19, 2013, accessed from <https://corporate.target.com/discover/article/Important-Notice-Unauthorized-access-to-payment-ca> on December 19, 2013.

<sup>7</sup> *Id.*

21. In contrast with Target's announcement on its corporate website, hackers obtained the information encoded on the magnetic stripe of cards known in the industry as "Magnetic Stripe Data" or "Track Data." The data encoded in the magnetic stripe is for authorization during card-present transactions. Unauthorized possession of this information is far more dangerous than possession of CVV codes alone, for having it enables miscreants to combine all of the elements necessary to create usable counterfeit cards. According to Krebs, "The type of data stolen – also known a 'track data' – allows thieves to create counterfeit cards be encoding the information onto any card with a magnetic stripe."<sup>8</sup> This means that criminals are able to create "clones" of the cards that were swiped at Target stores and use them to make fraudulent "card-present," or "card-not-present" debit or credit transactions with the accounts.

22. It is a violation of the terms of the PCI Data Security Standards, the Visa Operating Regulations, and the MasterCard Rules for Retailers, to store sensitive cardholder account authentication information beyond authorization. This information consists of: magnetic stripe or "track data," CVV2 data, or PIN data.<sup>9</sup>

23. Target may have stored magnetic stripe or "track data," CVV2 data, or PIN data, in violation of PCI Data Security Standards and Visa Operating Regulations. Indeed, on December 27, Target announced that debit card PINs were among the information stolen in the

---

<sup>8</sup> Krebs, Brian. *Sources: Target Investigating Data Breach*. December 13, 2013, retrieved from <http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/> on December 23, 2013.

<sup>9</sup> PCI Data Security Standard 3.2.2; Visa. *Visa Cardholder Information Security Program Prohibited Data Retention Attestation*, retrieved from [usa.visa.com/download/merchants/pdra\\_form\\_dec2006.doc](http://usa.visa.com/download/merchants/pdra_form_dec2006.doc) on December 25, 2013; MasterCard, *MasterCard Rules*, retrieved from [http://www.mastercard.com/us/merchant/pdf/BM-Entire\\_Manual\\_public.pdf](http://www.mastercard.com/us/merchant/pdf/BM-Entire_Manual_public.pdf) on December 30, 2013..

data breach: “a Target spokeswoman backtracked from previous statements and said criminals had made off with customers’ encrypted PIN information as well.”<sup>10</sup>

24. The damage caused by Target’s negligence is severe. Not only are its customers presently in peril of theft of their money and identities, the losses will continue for years to come. An offer by Target’s CEO Gregg Steinhafel for a two-day ten percent discount is too little, too late.<sup>11</sup>

25. Target failed to implement and maintain reasonable security procedures and practices to protect the nature and scope of the information stored by Target and as a result, the Personal Information of Plaintiffs and the other members of the Classes was compromised in the data breach.

26. Had Target devoted sufficient money and resources to maintain a secure network, hackers would have been unable to exploit flaws in Target’s computer infrastructure, and unable to so easily collect customers’ credit and debit card information. Unfortunately for Plaintiffs and the other Class members, Target instead chose the non-preventative approach described by Mark Rasch, a cybersecurity specialist and a former federal cybercrime prosecutor in Bethesda, Maryland: “Most merchants are content to clean up the damage from an attack, rather than pay for better preventive measures.”<sup>12</sup>

27. According to James Lyne, global head of security research for the computer security firm Sophos, something was obviously defective about Target’s security measures:

---

<sup>10</sup> Perloth, Nicole. *Target’s Nightmare Goes On: Encrypted PIN Data Stolen*. December 27, 2013, retrieved from <http://bits.blogs.nytimes.com/2013/12/27/targets-nightmare-goes-on-encrypted-pin-data-stolen> on December 28, 2013.

<sup>11</sup> Steinhafel, Greg. *A Message from CEO Gregg Steinhafel about Target’s Payment Card Issues*. December 20, 2013, retrieved from <http://www.abullseyeview.com/2013/12/ceomessage/> on December 24, 2013 (“We’re in this together, and in that spirit, we are extending a 10% discount – the same amount our team members receive – to guests who shop in U.S. stores on Dec. 21 and 22.”).

<sup>12</sup> Anderson, Craig. *Identity theft growing, costly to victims*. April 13, 2013, retrieved from <http://www.usatoday.com/story/money/personalfinance/2013/04/14/identity-theft-growing/2082179/> on December 24, 2013.

“Forty million cards stolen really shows a substantial security failure. This shouldn’t have happened.”<sup>13</sup>

28. Other security experts agree. For example, Forrester analyst John Kindervag indicated that “[t]his is a breach that should’ve never happened,” adding “the fact that three-digit CVV security codes were compromised shows they were being stored. Storing CVV codes has long been banned by the card brands and the PCI [Security Standards Council].” Further, InformationWeek information security reporter Mathew Schwartz wrote: “Reached via email, a Target official declined to respond to questions about whether the retailer had stored the stolen card data in encrypted format, or whether it had been certified as PCI-compliant.”<sup>14</sup>

29. It has already been reported that “credit and debit card accounts stolen in [the Target data breach] have been flooding underground black markets in recent weeks, selling in batches of one million cards and going for anywhere from \$20 to more than \$100 per card.”<sup>15</sup> Therefore, the Personal Information of Plaintiffs and other Class members is at great risk of being sold to criminals, if it has not been sold already.

30. Krebs reported that he obtained information from various bank sources who found cards issued by their respective banks for sale at underground card shops and were able to identify many of those cards as having been compromised in the Target data breach:

At least two sources at major banks said they’d heard from the credit card companies: More than a million of their cards were thought to have been compromised in the Target breach. One of those institutions noticed that one card shop in particular had recently alerted its loyal customers about a huge new

---

<sup>13</sup> Associated Press. *Answers to Questions about the Target data breach*. December 19, 2013, retrieved from [http://www.washingtonpost.com/business/technology/answers-to-questions-about-the-target-data-breach/2013/12/19/bde98d30-68d4-11e3-997b-9213b17dac97\\_story.html](http://www.washingtonpost.com/business/technology/answers-to-questions-about-the-target-data-breach/2013/12/19/bde98d30-68d4-11e3-997b-9213b17dac97_story.html) on December 23, 2013.

<sup>14</sup> Schwartz, Mathew. *Target Breach: 10 Facts*. January 21, 2013, retrieved from <http://www.informationweek.com/security/attacks-and-breaches/target-breach-10-facts/d/d-id/1113228> on December 25, 2013.

<sup>15</sup> Krebs, Brian. *Cards Stolen in Target Breach Flood Underground Markets*. December 20, 2013, retrieved from <http://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/> on December 24, 2013.

batch of more than a million quality dumps that had been added to the online store. Suspecting that the advertised cache of new dumps were actually stolen in the Target breach, fraud investigators with the bank browsed this card shop's wares and effectively bought back hundreds of the bank's own cards. When the bank examined the common point of purchase among all the dumps it had bought from the shady card shop, it found that all of them had been used in Target stores nationwide between Nov. 27 and Dec. 15. Subsequent buys of new cards added to that same shop returned the same result.<sup>16</sup>

31. Krebs also reported similar results from a smaller bank that had bought back twenty of its cards from a similar shop and found that while one of them had been cancelled, the remaining nineteen cards "had been used by customers to make purchases at Target stores around the country between Nov. 29 and Dec. 15," and that some of those cards "'already ha[d] confirmed fraud on them.'" (quoting his bank source).<sup>17</sup>

32. The seriousness of the intrusion into Target's network and the value of the data stolen in terms of its use for criminal activities cannot be understated, and consumers around the nation are already experiencing unauthorized transactions and theft of funds as a result of Target's failures to safeguard and control its cardholder data environment.


33. Scores of scared and angry Target customers sounded off on Target's Facebook page, describing how the data breach wreaked havoc on their financial lives during the busy holiday season, complaining of unauthorized transactions, irritation, and expense associated with cancelling cards, and expressing frustration over their inability to reach Target customer support.<sup>18</sup> Examples of actual customer comments on Target's Facebook page, with names and faces redacted, are reproduced below:

---

<sup>16</sup> *Id.*


<sup>17</sup> *Id.*

<sup>18</sup> Target's Facebook Page. December 21, 2013, retrieved from <https://www.facebook.com/target?fref=ts> on December 25, 2013.


 Well..... I shopped at TARGET during the security breach , and guess what...checking account drained today. Bank Of America caught it before I did, and they were very careful on what they said as far as the cause. Issuing a new card in 2-3 business days, and have to contact the fraud department in the same time frame to clean up the mess.... Happy Holidays from Target!

 View more comments


252 of 575

 I found out at 1am today that I had a charge on my account making me go negative just 2 days before Christmas! I had to cancel my debit card, now what do I use in the mean time?! This is a horrible time for this. The only thing we get to reimburse us is 10% (big whoop) off and that was only for 2 days (Dec 21 and 22)?! I just found out this happened and it is past those 2 days, so I can't even use the discount, not that I would be able to anyways with no money in my account and no debit card! I am do beyond disappointed and frustrated at Target!


Like · Reply · Yesterday at 11:04 via mobile

 Target claims to have resolved this issue, on Saturday 12/21/2013 I made a purchase. On Sunday my son asked me to check the balance on his account. That's when I noticed that \$144.00 had been charged on my account. Target has not resolved this issue, so buyer beware and use cash!


Like · Reply · Yesterday at 09:23 via mobile

 Walmart notified us that they cancelled a delivery because billing and shipping address didn't match / We never ordered anything from Walmart ... Thanks Target someone has our credit card info !!!




Like · Reply · 22 December at 17:27 via mobile




 My debit card was hacked and a purchase of \$439 was made at a Brooklyn New York target!! I live in the south. I went to my bank this morning. They canceled that card. I will get the money back in about 10 days. I really could have used that money during the holidays!!! Also, the 10% employee discount they are offering, well I didn't know my card was hacked until today!! So, I guess I don't get that either



Like · Reply · 6 · Yesterday at 14:30 via mobile




 Thanks Target for ruining my holiday ! I have been calling for days to cancel my card and haven't been able to get through . This is outrageous that you put us at risk for fraud and identity theft and can't even offer enough customer support to help us in need . And offering 10% off to everyone including the people not affected by this breach is a slap in the face . Thanks for nothing !!

Like · Reply · 3 · Yesterday at 19:31 via mobile

  Five days after the announcement (and apparently ten days after Target learned of the problem) I STILL can't get through on the phone. I've been trying frequently every day, but all I get is busy signals, dropped connections, and occasionally a recording. It should be possible to talk to a person by now. BTW, the reason I want to talk to someone is because I want to put a "hold" on my Redcard, which can't be done through the website. I don't want to cancel it because I have a balance and might have Christmas returns, but I don't want any additional charges to it now.  
Like · Reply ·  3 · Yesterday at 18:49

  You cannot call Target RedCard, the line is continually busy. You cannot sign on to your account online because it says "an error has occurred, please call". This is lousy customer service. How do I find out if my card is compromised if your customer service stinks so bad I can't even contact you. This is disgusting service.  
Like · Reply ·  1 · Yesterday at 12:26

  Well my family's bank account was hit. I apparently bought stuff for a crook in Utah. Pretty unhappy Target.  
Like · Reply · Yesterday at 22:54 via mobile

  Nothing like having your card canceled because someone stole your info on black Friday while shopping at target. At least they caught the transaction before they were able to take \$100 out of my account all the way in San Antonio Texas. It's really going to suck not having my debit card for last minute Christmas shopping.  
Like · Reply ·  1 · Yesterday at 21:39 via mobile

34. Target's failure to directly notify its customers affected by the data breach may have violated the provisions of Massachusetts General Laws, Chapter 93H, and in particular the reporting provisions of c. 93H, § 3, which required Target, once it knew or had reason to know of a data security breach involving personal information and affecting Massachusetts residents, to provide prompt and direct notice of such breach to any affected Massachusetts residents, to the Massachusetts attorney general, and to the director of consumer affairs and business regulation for Massachusetts. Target's failure to provide direct notice may also have violated various other similar state statutes. *See, e.g.*, Cal. Civ. Code § 1798.82 (California); HRS § 487N-2 (Hawaii); 815 ILCS 530/10 (Illinois); La. R.S. § 51:3074 (Louisiana); Minn. Stat. §

325E.61 (Minnesota); N.C.Gen. Stat. § 75-65 (North Carolina); R.I. Gen. Laws § 11-49.2-3 (Rhode Island); Tenn. Code Ann. § 47-18-2107 (Tennessee); and Rev. Code Wash. § 19.255.010 (Washington).

35. Target's failure to keep Class members' data secure has had and will continue to have severe and long-lasting consequences for the members of the Classes, including Plaintiffs, because the loss of data encoded in the magnetic strip of credit and debit cards gives rise to various forms of theft and fraud:

The most common form [of identity theft] however, involves credit card accounts. This occurs when an identity thief obtains either the actual credit card, the numbers associated with the account, or the information derived from the **magnetic strip** on the back of the card. Because it is possible to make charges through remote purchases, such as online sale or by telephone, identity thieves are often able to commit fraud even as the card remains in the consumer's wallet.<sup>19</sup> (emphasis added).

36. Victims of credit card fraud often have to expend considerable time and money to repair the damage caused. For example, when an identity thief opens up a new account using a victim's personal information, that victim must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.<sup>20</sup>

37. Identity thieves create additional adverse consequences by opening unauthorized accounts, taking out loans, and stealing funds. The effects can be long-lasting and devastating: "when a stolen identity is used to apply for additional lines of credit, the victim can spend years trying to resolve bad debt run up by thieves in their names. Some struggle to borrow money

---

<sup>19</sup> *The President's Identity Theft Task Force Report*. April, 2007, retrieved from <http://www.idtheft.gov/reports/StrategicPlan.pdf> on December 24, 2013.

<sup>20</sup> *Id.*

because of the damage to their credit scores. Others have been forced to file bankruptcy and lose their homes.”<sup>21</sup>

38. According to a U.S. Government Accountability Office study regarding data breaches, “stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.”<sup>22</sup> The pilfered credit card data in this case reached the global marketplace rapidly.<sup>23</sup>

39. Victims of the Target data breach who take the preventative measure of cancelling their cards will experience delays in accessing their funds while they wait for replacement cards to arrive.

40. Plaintiffs and the Classes now face years of constant surveillance of their financial and personal records, in addition to emotional distress and financial losses they have incurred, or will incur.

## **V. CLASS ACTION ALLEGATIONS**

41. Plaintiff Casey brings this action on his own behalf, and on behalf of the following class (the “Massachusetts Class”):

All persons who used credit or debit cards at Target stores in Massachusetts and whose personal and/or financial information was breached during the period from on or about November 27 to on or about December 15, 2013. Excluded from the Class are Defendant; officers and employees of Defendant; any entity in which Defendant has a

---

<sup>21</sup> Anderson, Craig. *Identity theft growing, costly to victims*. April 13, 2013, retrieved from <http://www.usatoday.com/story/money/personalfinance/2013/04/14/identity-theft-growing/2082179/> on December 24, 2013.

<sup>22</sup> Government Accounting Office. *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*. June 2007, retrieved from <http://www.gao.gov/assets/270/262904.html> on January 24, 2013.

<sup>23</sup> Krebs, Brian. *Who’s Selling Credit Cards From Target?* December 20, 2013, retrieved from <http://krebsonsecurity.com/2013/12/whos-selling-credit-cards-from-target/> on December 25, 2013.

controlling interest; the affiliates, legal representatives, attorneys, heirs, and assigns of the Defendant.

42. Plaintiffs R. Hauss and S. Hauss bring this action on their own behalf, and on behalf of the following class (the "Ohio Class"):

All persons who used credit or debit cards at Target stores in Ohio and whose personal and/or financial information was breached during the period from on or about November 27 to on or about December 15, 2013. Excluded from the Class are Defendant; officers and employees of Defendant; any entity in which Defendant has a controlling interest; the affiliates, legal representatives, attorneys, heirs, and assigns of the Defendant.

43. Each Class satisfies the requirements of Fed. R. Civ. P. 23(a), 23(b)(2) and 23(b)(3), and their claims are appropriate for class treatment.

44. **Numerosity:** The members of each of the Classes are so numerous that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiffs at this time, based on information and belief, it is in the millions. Target operates 36 retail store locations in Massachusetts, and of the 40 million card accounts stolen in the data breach, approximately one million of those accounts belonged to customers who made purchases at the Massachusetts stores. Target also operates 64 retail store locations in Ohio.

45. **Commonality and Predominance:** There are questions of law and fact common to all members of each Class, and those questions predominate over questions affecting only individual Class members. Those common questions include

- a. Whether Defendant unlawfully used, maintained, lost or disclosed Class members' personal and/or financial information;
- b. Whether Target unreasonably delayed in notifying members of the Classes of the data breach;

- c. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information stored and compromised in the data breach;
- d. Whether Defendant's conduct was negligent;
- e. Whether Defendant's conduct violated Class members' right to privacy;
- f. Whether Plaintiffs and the Classes are entitled to damages, civil penalties, and/or injunctive relief.

46. **Typicality:** Plaintiffs' claims are typical of those of other members of the Class they seek to represent because Plaintiffs' Personal Information, like that of every other Class member, was misused and/or disclosed by Defendant.

47. **Adequacy:** Plaintiffs will fairly and adequately represent the interests of their respective Classes. Plaintiffs have retained counsel who are competent and experienced in class actions and complex consumer litigation, and there are no conflicts between the interests of the Plaintiffs and the interest of the Classes that they seek to represent.

48. **Superiority:** The prosecution of separate actions by individual members of each Class would create a risk of inconsistent or varying adjudications with respect to individual members of each Class, which would establish incompatible standards of conduct for Defendant and would lead to repetitive adjudication of common questions of law and fact. Accordingly, class treatment is superior to any other method for adjudicating this controversy. Plaintiffs know of no difficulty that will be encountered in the management of this litigation that would preclude its maintenance as a class action under Rule 23(b)(3).

49. Defendant has acted or refused to act on grounds that apply generally to each Class, so that final injunctive relief or corresponding declaratory relief is appropriate with respect to each Class as a whole.

## **VI. CAUSES OF ACTION**

### **COUNT ONE**

#### **Invasion of Privacy Under M.G.L. c. 214, § 1B (brought by Plaintiff Casey on behalf of the Massachusetts Class)**

50. Casey incorporates the substantive allegations contained in all previous paragraphs as if fully set forth herein.

51. Casey and the Massachusetts Class had a reasonable expectation of privacy in the Personal Information Defendant mishandled.

52. By failing to keep Casey's and the other Massachusetts Class members' Personal Information safe and secure, and by misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant invaded Casey's and the other Massachusetts Class members' privacy. This invasion of privacy was unreasonable and was substantial and serious.

53. Defendant invaded Casey's and the Massachusetts Class's right to privacy and intruded into their private affairs by misusing and/or disclosing Casey's and the Massachusetts Class's Personal Information without their informed, voluntary, affirmative and clear consent.

54. As a proximate result of such misuse and disclosures, Casey's and the Massachusetts Class's reasonable expectations of privacy in their Personal Information was violated. Casey and the other members of the Massachusetts Class incurred damages as a result of Defendant's invasion of privacy.

## **COUNT TWO**

### **Invasion of Privacy (On behalf of the Massachusetts and Ohio Classes)**

55. Plaintiffs incorporate the substantive allegations contained in all previous paragraphs as if fully set forth herein.

56. Plaintiffs and the Classes had a reasonable expectation of privacy in the Personal Information that Defendant mishandled.

57. By failing to keep Plaintiffs' and other Class members' Personal Information safe and secure, and by misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant invaded Plaintiffs' and the other Class members' privacy.

58. Defendant invaded Plaintiffs' and each Class's right to privacy and unreasonably intruded into their private affairs by misusing and/or disclosing Plaintiffs' and each Class's Personal Information without their informed, voluntary, affirmative and clear consent.

59. As a proximate result of such misuse and disclosures, Plaintiffs' and each Class's reasonable expectations of privacy in their Personal Information was violated. Plaintiffs and the members of each Class incurred damages as a result of Defendant's invasion of privacy.

## **COUNT THREE**

### **Negligence (On behalf of the Massachusetts and Ohio Classes)**

60. Plaintiffs incorporate the substantive allegations contained in all previous paragraphs as if fully set forth herein.

61. Defendant owed a duty to Plaintiffs and the other members of the respective Classes to exercise reasonable care in safeguarding and protecting their Personal Information in its possession from being compromised, lost, stolen, misused and/or disclosed to unauthorized

parties. This duty included among other things, designing, maintaining and testing Defendant's security systems to ensure that Plaintiffs' and the other Class members' Personal Information in Defendant's possession was adequately secured and protected, and to use reasonable care to destroy, and not unnecessarily store their Personal Information. Defendant also had a duty to implement processes that would detect a breach of its security system in a timely manner.

62. Defendant had a duty to timely disclose to Plaintiffs and the other members of the respective Classes that their Personal Information had been or was reasonably believed to be compromised. Timely disclosure would allow Plaintiffs and the other members of the respective Classes to take appropriate action to avoid unauthorized charges on their accounts and unauthorized disbursements of funds from their bank accounts; cancel or change account numbers on the compromised credit and debit cards; and monitor their account information for fraudulent charges.

63. Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiffs' and the other Class members' Personal Information in its possession by failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and the other Class members' Personal Information; failing to adequately monitor the security of its network and cardholder data environment; allowing unauthorized access to Plaintiffs' and the other Class members' Personal Information stored on its network and cardholder data environment; improperly storing Personal Information on its network and cardholder data environment; and failing to recognize in a timely manner that its network had been breached. Defendant's actions were in violation of, among other things, industry standards, practices, rules and regulations.

64. Defendant breached its duty to timely disclose that Plaintiffs' and the other Class members' Personal Information in its possession had been or was reasonably believed to have been, stolen or compromised.

65. The breach of security and unauthorized access to the Plaintiffs' and the other Class members' Personal Information was reasonably foreseeable as a result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and the other Class members' Personal Information.

66. As a direct and proximate result of the Defendant's conduct, each Class suffered damages including, but not limited to, loss of control of their Personal Information; monetary loss for fraudulent charges and unauthorized disbursements; fear and apprehension of fraud, loss of money and identity theft; the burden and cost of credit monitoring to monitor their accounts and credit history; the burden and cost of closing compromised accounts and opening new accounts; the burden of closely scrutinizing statements for past and future transactions; damage to their credit standing; loss of privacy; and other economic and non-economic damages.

#### **COUNT FOUR**

##### **Negligent Misrepresentation (On behalf of the Massachusetts and Ohio Classes)**

67. Plaintiffs incorporate the substantive allegations contained in all previous paragraphs as if fully set forth herein.

68. Defendant assumed a duty to use reasonable care to ensure the security of Plaintiffs' and the other Class members' Personal Information.

69. In the course of the operation of Defendant's business as a retail store, Defendant negligently misrepresented that Plaintiffs' and the other Class members' Personal Information

was safe and secure. This representation was false – the Personal Information of Plaintiffs and the other Class members was anything but secure. Indeed, the Personal Information was compromised in a massive security breach, and much of the Personal Information has been or will be used by thieves to steal money from Plaintiffs and the other Class members.

70. Furthermore, Defendant failed to exercise reasonable care or competence in identifying the breach and communicating the information about the breach to Plaintiffs and the other Class members, and thereby Defendant failed to correct its negligent misrepresentation that the Personal Information was secure. Indeed, as alleged above, Defendant waited *four days* after discovering the breach before reporting the breach to Plaintiffs and the other Class members.

71. Plaintiffs and the other Class members reasonably relied on Defendant's negligent misrepresentation that the Personal Information would be kept safe and secure when Plaintiffs and the other Class members provided Defendant with the information.

72. As a direct and proximate result of Plaintiffs' and the other Class members' justified reliance on Defendant's negligent misrepresentation, Plaintiffs and the other Class members have suffered damages including, but not limited to, loss of control of their credit card and other personal financial information; monetary loss for fraudulent charges incurred on their accounts; fear and apprehension of fraud and loss of money; the burden and cost of credit monitoring to monitor their accounts and credit history; the burden and cost of closing compromised accounts and opening new accounts; the burden of closely scrutinizing credit card statements for past and future transactions; damage to their credit history; loss of privacy; and other economic damages.

## **COUNT FIVE**

### **Breach of Implied Contract (On behalf of the Massachusetts and Ohio Classes)**

73. Plaintiffs incorporate the substantive allegations contained in all previous paragraphs as if set forth herein.

74. When they confided their private and confidential debit and credit card information to Defendant in order to make purchases at Defendant's stores, Plaintiffs and the other Class members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect all such information and to notify Plaintiffs and the other members of the respective Classes in the event that the confidentiality of such information was compromised.

75. Plaintiffs and the other Class members would not have entrusted their private and confidential information financial and personal information to Defendant in the absence of such an implied contract with Defendant.

76. Defendant breached the implied contracts they made with Plaintiffs and the other Class members by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information.

77. The damages sustained by Plaintiffs and the other Class members as described above were the direct and proximate result of Defendant's breaches of these implied contracts.

## **VII. PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs, on behalf of themselves and the Classes, pray for the following relief:

- A. An order certifying each Class as defined above;
- B. An award of actual and statutory damages;

C. An injunction requiring Defendant to correct all flaws in its cardholder data environment;

D. Equitable relief enjoining the Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and the other Class members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to the Plaintiffs and the other Class members;

E. An award of reasonable attorneys' fees and costs; and

F. Such further and other relief as the Court deems reasonable and just.

### **VIII. JURY DEMAND**

Plaintiffs request a trial by jury of all claims that can be so tried.

Dated: December 31, 2013

Respectfully submitted,

**PASTOR LAW OFFICE, LLP**  
/s/ David Pastor (BBO # 391000)  
63 Atlantic Avenue, 3d Floor  
Boston, MA 02110  
Telephone: 617-742-9700  
Facsimile: 617-742-9701  
*Dpastor@pastorlawoffice.com*

**LEONARD LAW OFFICE, LLP**  
/s/ Preston W. Leonard (BBO # 680991)  
139 Charles St., Suite A121  
Boston, MA 02114  
Telephone: 617-329-1295  
*Pleonard@theleonardlawoffice.com*

**WOLF HALDENSTEIN ADLER  
FREEMAN & HERZ, LLP**  
/s/Janine L. Pollack  
/s/Stacey Kelly Breen  
/s/ Lydia Keaney Reynolds  
270 Madison Avenue  
New York, NY 10016  
Telephone: 212-545-4600  
*Pollack@whafh.com*  
*Breen@whafh.com*  
*Reynolds@whafh.com*

*Counsel for Plaintiffs and the Class*